PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-300560
(43)Date of publication of application : 11.10.2002

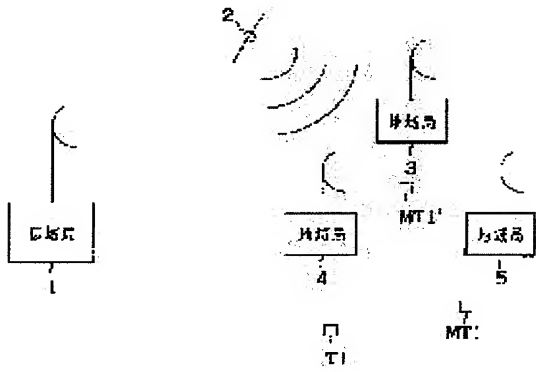
(51)Int.Cl. H04N 7/16
H04H 1/00
H04L 9/08

(21)Application number : 2001-101420
(22)Date of filing : 30.03.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : AKIYAMA KOICHIRO

(54) LIMITED RECEPTION SYSTEM, WIDE-AREA STATION CONTRACT CONTROLLER, AND LOCAL STATION CONTRACT CONTROLLER

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the quantity of transmission of limited reception information.
SOLUTION: A wide-area station 1 broadcasts the broadcast contents and the information relevant to programs by wide area broadcasting, which performs broadcasting over a relatively wide range. Moreover, the wide-area station 1 broadcasts information, relevant to channel contract having described the contract conditions for each channel for performing limited reception, for local stations 3, 4, and so on. The local stations 3, 4, and so on broadcast this information within their own broadcast ranges, when they receive the information relevant to the channel contracts addressed to subscribers within own stations. Hereby, the increase of the quantity of broadcast is suppressed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－300560
（P2002－300560A）
(43)公開日　平成14年10月11日(2002.10.11)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04N 7/16		H04N 7/16	Z	5C064
H04H 1/00		H04H 1/00	U	5J104
			B	
H04L 9/08		H04L 9/00	601B	
			601D	

審査請求　未請求　請求項の数10　ＯＬ　（全 19 頁）　最終頁に続く

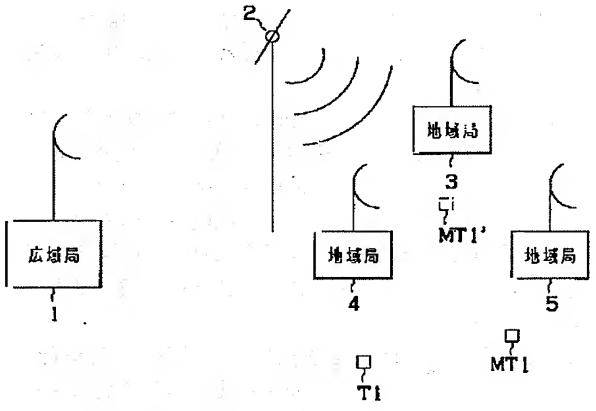
(21)出願番号　特願2001－101420(P2001－101420)
(22)出願日　平成13年３月30日(2001.3.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100076233
弁理士　伊藤　進

最終頁に続く

(54)【発明の名称】　限定受信システム、広域局契約管理装置及び地域局契約管理装置

(57)【要約】
【課題】限定受信情報の送信量を低減する。
【解決手段】広域局１は、放送コンテンツ及び番組関連情報については比較的広範囲に放送を行なう広域放送によって放送する。また、広域局１は、限定受信を行なうためにチャネル毎の契約状態を記述したチャネル契約関連情報については、地域局３，４，…宛に放送する。地域局３，４，…は、自局内の加入者宛チャネル契約関連情報を受信すると、この情報を自局の放送範囲内に地域放送する。これにより、送信量の増大が抑制される。



【特許請求の範囲】
【請求項１】　コンテンツ情報を放送する広域放送局と、
前記コンテンツ情報を利用する契約した受信端末と、
前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、前記広域放送局の放送範囲よりも狭い放送範囲に放送する地域放送局とを具備したことを特徴とする限定受信システム。
【請求項２】　前記地域放送局は、地方局、中継局又はギャップフィラーであることを特徴とする請求項１に記載の限定受信システム。
【請求項３】　前記地域放送局は、前記広域放送局が放送した契約関連情報を受信して、自放送範囲内に加入している前記受信端末に放送することを特徴とする請求項１に記載の限定受信システム。
【請求項４】　前記地域放送局は、前記広域放送局が通信によって送信した契約関連情報を受信して、自放送範囲内に加入している前記受信端末に放送することを特徴とする請求項１に記載の限定受信システム。
【請求項５】　契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送手段と、
前記広域放送手段の放送範囲よりも狭い放送範囲に放送する複数の地域放送局に対して、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、宛先を指定して送信する契約関連情報送信手段と具備したことを特徴とする広域局契約管理装置。
【請求項６】　前記契約関連情報送信手段は、前記複数の地域放送局に対して、放送又は通信によって前記契約関連情報を送信することを特徴とする請求項５に記載の広域局契約管理装置。
【請求項７】　前記地域放送局は、地方局、中継局又はギャップフィラーであることを特徴とする請求項５に記載の広域局契約管理装置。
【請求項８】　契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送局から、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報が与えられ、前記広域放送局の放送範囲よりも狭い放送範囲に前記受信端末毎の契約関連情報を放送する地域放送手段を具備したことを特徴とする地域局契約管理装置。
【請求項９】　前記地域放送手段は、前記広域放送局から、放送又は通信によって前記契約関連情報を受信することを特徴とする請求項８に記載の地域局契約管理装置。
【請求項１０】　前記地域放送手段は、地方局、中継局又はギャップフィラーであることを特徴とする請求項８に記載の地域局契約管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、たとえば、契約内容に応じて放送配信されるコンテンツを復号する有料放送サービスの契約関連情報の送信を効率化した限定受信システム、広域局契約管理装置及び地域局契約管理装置に関する。
【０００２】
【従来の技術】近年、放送のデジタル化が進んでいる。通信衛星（ＣＳ）に始まり、ケーブルＴＶ、地上放送へと進んだデジタル放送は、一層のサービスの充実とともに、これからの放送サービスの主役をつとめていくものと思われる。
【０００３】デジタル放送の最大の特徴は、情報圧縮技術の導入によって番組の送信に要する周波数の使用効率が向上し、アナログ放送に比較して放送チャネル数が大幅に増加したことである。更に、デジタル放送では、高度な誤り訂正技術を適用することができ、高品質で均質なサービスの提供が可能となる。
【０００４】また、デジタル化によって、従来のような画像や音声による放送だけでなく、文字やデータによる放送（データ放送）も可能になり、例えばニュースを文字データとして放送することや、ＰＣ（パーソナルコンピュータ）ソフトを放送で配信することも可能となり、これらのサービスを提供するためのシステムも続々登場してきている。
【０００５】ところで、有料放送サービスでは、番組の不正視聴を防止するために番組にスクランブルが施される。スクランブルを利用した有料放送では、契約内容に基づいたスクランブルの解除及び復号が受信機で可能なように、契約期間に即した顧客管理を行う必要がある。契約期間に即した顧客管理によって、例えば、所定の料金の支払による契約期間内に限って契約チャネルの番組の視聴を許可することが可能となる。
【０００６】不正視聴を防止する点から、受信装置にてスクランブルあるいは暗号を解くための鍵情報（限定受信情報）は、正当な視聴者のみに、契約チャネル、契約期間に即して、確実に提供されるようにする必要がある。
【０００７】図３４はデジタル放送において採用される鍵構成の一例を示す説明図である。図３４に示すマスター鍵ＫＭは、放送受信装置に固有の鍵である。送信側では、図３４の矢印に示すように、チャネルキーＫchを用いて放送コンテンツをスクランブルする。そして、各チャネルに固有のワーク鍵Ｋｗを用いて、スクランブルされた放送コンテンツ及びチャネルキーＫchを暗号化して送信する。
【０００８】一方、ワーク鍵Ｋｗは、マスター鍵ＫＭによってチャネル契約関連情報と共に暗号化されて送信される。チャネル契約関連情報はチャネル毎の契約期間又は契約の有無等の情報である。なお、ワーク鍵Ｋｗは、契約最小期間（例えば１ヶ月）毎に更新される。
【０００９】ワーク鍵Ｋｗ及びチャネル契約関連情報

は、受信側において、コンテンツの受信に先だって受信されて蓄積される。コンテンツ視聴時はチャネル契約関連情報を参照して、チャネルの視聴可否を判断し、ワーク鍵Kw を用いて受信チャネルのチャネルキーKchを復号する。チャネルキーKchによって、スクランブルされた放送コンテンツをデスクランブルする。

【００１０】このように、図３４の鍵構成を採用するデジタル放送方式では、有料放送の実現のために、契約者毎にチャネル契約関連情報と該チャネル契約関連情報に見合ったチャネルのワーク鍵Kw を定期的に送信している。しかし、契約最小期間毎に契約者個別にワーク鍵を送信しなければならず、契約者の増加等によって、このような限定受信情報の送信量も増大し、その送信は困難になりつつある。

【００１１】

【発明が解決しようとする課題】このように、従来、有料放送等の限定受信システムを可能にするためには、復号に用いるワーク鍵を定期的に放送する必要があり、契約者の増加等によって送信量が増大してしまうという問題点があった。

【００１２】本発明はかかる問題点に鑑みてなされたものであって、限定受信に必要な情報の放送を効率化することにより、送信量の増大を抑制することができる限定受信システム、広域局契約管理装置及び地域局契約管理装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】本発明の請求項１に係る限定受信システムは、コンテンツ情報を放送する広域放送局と、前記コンテンツ情報を利用する契約した受信端末と、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、前記広域放送局の放送範囲よりも狭い放送範囲に放送する地域放送局とを具備したものであり、本発明の請求項５に係る広域局契約管理装置は、契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送手段と、前記広域放送手段の放送範囲よりも狭い放送範囲に放送する複数の地域放送局に対して、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報を、宛先を指定して送信する契約関連情報送信手段と具備したものであり、本発明の請求項８に係る地域局契約管理装置は、契約した受信端末の利用に供するためにコンテンツ情報を放送する広域放送局から、前記コンテンツ情報の利用を制御するために前記契約した受信端末毎の契約関連情報が与えられ、前記広域放送局の放送範囲よりも狭い放送範囲に前記受信端末毎の契約関連情報を放送する地域放送手段を具備したものである。

【００１４】本発明の請求項１において、広域放送局は、コンテンツ情報を放送する。コンテンツ情報の利用を制御するために受信端末毎の契約関連情報は、広域放送局の放送範囲よりも狭い放送範囲に放送する地域放送局によって放送される。受信端末は地域放送局の放送によって契約関連情報を受信し、これにより、受信端末は、コンテンツ情報を受信して利用する。

【００１５】本発明の請求項５において、広域放送手段は、契約した受信端末の利用に供するためにコンテンツ情報を放送する。契約関連情報送信手段は、広域放送手段の放送範囲よりも狭い放送範囲に放送を行う複数の地域放送局に対して各宛先を指定して、コンテンツ情報の利用を制御するために受信端末毎の契約関連情報を送信する。

【００１６】本発明の請求項８において、地域放送手段は、広域放送局から、コンテンツ情報の利用を制御するための受信端末毎の契約関連情報が与えられて、広域放送局の放送範囲よりも狭い放送範囲に受信端末毎の契約関連情報を放送する。

【００１７】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。図１は本発明に係る限定受信システムの一実施の形態を示す説明図である。本実施の形態は受信機の固有のマスター鍵を用いる限定受信システムに適用したものである。

【００１８】本実施の形態は衛星放送等を使って比較的広範囲に放送を行なう広域放送によって放送コンテンツを放送すると共に、チャネル毎の契約状態を記述したチャネル契約関連情報については、地上波等を使って比較的狭い範囲に放送を行なう地方放送等の地域放送によって放送することを可能にすることにより、送信量の増大を抑制するようにしたものである。

【００１９】先ず、図２乃至図６を参照して、限定受信システムにおいて伝送される情報について説明する。

【００２０】本実施の形態においては、各受信装置が個別のマスター鍵を有する場合の例を示している。即ち、本実施の形態では、図３４と同様の鍵構成が採用される。

【００２１】上述したように、このシステムでは、各受信装置に対して、定期的にしかも個別にチャネル契約関連情報を暗号化して送信する必要があり、送信量が増大する。しかしその反面、マスター鍵が不正入手された場合の被害範囲が狭く安全性が高い。なお、以下に述べる限定受信方式は、社団法人電波産業会が策定したＢＳデジタル放送限定受信方式の標準規格のＡＲＩＢ　ＳＴＤ－Ｂ２５　１．０版（以下、ＡＲＩＢ規格という）に則った方式を簡明に説明したものである。

【００２２】放送局が放送する放送コンテンツは、チャネルキーKchを使って慣用暗号方式で暗号化される。更に、スクランブルされた放送コンテンツ及びチャネルキーKchは、各チャネルに固有のワーク鍵Kw を用いて暗号化される。

【００２３】チャネルキーKchは解読を防ぐため通常１０分程度の短時間で変更する必要がある。従って、チャ

ネルキーKchを個別のマスター鍵を用いて暗号化すると、送信量が膨大となる。そこで、全受信装置に共通のワーク鍵Kw でチャネルキーKchを暗号化するのである。

【００２４】また、同一のワーク鍵Kw を何カ月もの期間連続して使用すると、不正に解読される虞が高くなる。そこで、不正視聴を防止するために、視聴契約の変更時だけでなく適宜のタイミングでワーク鍵Kw を変更するようになっている。このため、放送コンテンツの復号に必要なワーク鍵Kw についても、多重化して受信側に送信する。この場合、ワーク鍵Kchについては受信機に固有のマスター鍵KMで暗号化して送信する。例えマスター鍵KM が不正に入手された場合でも、ワーク鍵Kw を変更することによって無料視聴を防止することができる。

【００２５】本実施の形態の限定受信システムにおいて放送受信装置が受信するデータは、コンテンツパケット、番組関連情報パケット、契約関連情報パケットの３種類である。

【００２６】図２乃至図４は夫々コンテンツパケット、番組関連情報パケット及び契約関連情報パケットのパケット形式を示す説明図である。図２乃至図４において［］で囲ったデータは、スクランブル又は暗号化されたデータを示している。

【００２７】図２に示すように、コンテンツパケットは、情報識別子、チャネル識別子、チャネルキー識別子、放送コンテンツによって構成される。情報識別子は、当該パケットの種別を示すもので、コンテンツパケットであることを示す識別子が記述される。チャネル識別子は、当該放送コンテンツがいずれのチャネルのコンテンツであるかを示すものである。

【００２８】また、チャネルキー識別子は、当該放送コンテンツを復号するチャネルキーKchの識別子を示す。放送コンテンツは生の番組データで、チャネルキー識別子で指定されたチャネルキーKchで暗号化されている。なお、本実施の形態ではこれら全ての情報は固定長で表現されたデータであるものとする。

【００２９】図３に示すように、番組関連情報パケットは、情報識別子、チャネル識別子、ワーク鍵識別子、チャネルキー識別子、チャネルキーKchによって構成される。情報識別子は当該パケットの種別を示すもので、番組関連情報パケットであることを示す識別子が記述される。

【００３０】チャネル識別子は当該番組関連情報がいずれのチャネルのものかを示すものである。また、ワーク鍵識別子は当該番組関連情報パケットがいずれのワーク鍵Kw によって暗号化されているかを示す情報である。チャネルキー識別子は次に記述されているチャネルキーの識別子であり、チャネルキーKchはチャネル識別子で指定されているチャネルの放送コンテンツの暗号化に使われているチャネルキーKchを示している。本実施の形態ではこれら全ての情報は固定長で表現されたデータであり、チャネルキー識別子からチャネルキーKchまでのデータがワーク鍵識別子で指定されたワーク鍵で暗号化されている。

【００３１】なお、図３の番組関連情報パケットは、上述したＡＲＩＢ規格におけるＥＣＭ（Entitlement Control Message）に相当する。

【００３２】図４に示すように、契約関連情報パケットは、情報識別子、受信装置ＩＤ、ワーク鍵情報、チャネル契約関連情報Ｃ、誤り検出コードによって構成されている。情報識別子は当該パケットの種別を示すもので、契約関連情報パケットであることを示す識別子が記述される。受信装置ＩＤは当該契約関連情報がいずれの受信装置宛てのものであるかを示すものである。

【００３３】ワーク鍵情報は、当該受信者が契約しているチャネルのワーク鍵についての情報である。図５はワーク鍵情報の形式を示す説明図である。図５に示すように、ワーク鍵情報は、ワーク鍵の数ｎとそれに続くｎ個のチャネル識別子、ワーク鍵識別子、ワーク鍵の組で構成されている。

【００３４】チャネル契約関連情報Ｃは当該契約受信装置の契約状態を示すチャネル契約関連情報である。図６のビット列はチャネル契約関連情報を示している。チャネル契約関連情報は、限定受信を行なうためチャネル毎の契約状態を記述したものである。例えば、各チャネルにチャネル番号を付け、図６に示すように、チャネル番号に対応したビット（契約フラグ）が“１”であるか否かによってチャネルの契約状態を示している。図６の例では、契約フラグが“１”である第２、第５、第７、第８チャネルが契約済であることを示している。

【００３５】誤り検出コードはチャネル契約関連情報の誤りを検出するためのコードである。本実施の形態では契約関連情報パケット中の全ての情報は固定長で表現されたデータであり、ワーク鍵情報から誤り検出コードまでが受信装置ＩＤに対応した受信装置のマスター鍵で暗号化されている。

【００３６】なお、図４の契約関連情報パケットは、上述したＡＲＩＢ規格におけるＥＭＭ（Entitlement Management Message）に相当する。

【００３７】本実施の形態においては、図２のコンテンツパケット及び図３の番組関連情報パケットについては広域放送を行う広域局によって放送し、図４の契約関連情報パケットについては地域放送を行う地方放送局等の地域局によって放送するようになっている。

【００３８】なお、契約関連情報パケットについては比較的狭い範囲に放送を行なう放送局によって放送すればよく、地域局として、独自には番組制作を行なわない広域放送の再送信設備である中継局を採用して放送を行ってもよい。中継局の多くは、無人で運営されている。

【００３９】近年、自動車向けのデジタル放送においては、ギャップフィラーと呼ばれる中継局が採用される。モバイル受信装置に対して放送送信を行なうシステムにおいては、受信装置が移動することから、例えば都市部のビルの谷間等のような不感地域が生ずる。このため受信障害が起きるような地域のビルの屋上等にギャップフィラーを設け、衛星又は通信放送によって送信された放送波をギャップフィラーで受信し、当該地域向けに再送信するのである。本実施の形態においては、契約関連情報パケットの送信にギャップフィラーを利用可能である。

【００４０】次に、コンテンツパケット、番組関連情報パケット及び契約関連情報パケットを受信して、希望する番組の視聴を行う受信装置について説明する。図７は受信装置の全体構成を示すブロック図である。図８乃至図１１は受信装置の作用を説明するためのフローチャートである。図８乃至図１１において符号Ａ～Ｃは処理の連結を示している。

【００４１】図８は受信アルゴリズムを示すフローチャートである。受信装置１１は、受信信号をデスクランブルするデスクランブラを有していると共に、デスクランブルに必要なスクランブル鍵を発生するための限定受信チップ１７を備えている。限定受信チップ１７は、受信装置１１内部で限定受信の仕組みを実現するハードウェアであり、限定受信のための秘密情報が含まれているので内部のメモリやハード構成に関して外部から容易に読み出し、書き込み又は変更が不能な耐タンパ構造を有しているものとする。

【００４２】受信装置１１は、図８のステップS1 で、受信部１２によって放送波を受信する。Ａ／Ｄ変換部１３は受信した放送波をＡ／Ｄ変換してデジタルデータに変換する（ステップS2 ）。デジタルデータは誤り検出／訂正部１４に与えられて誤り検出／訂正が行われた後（ステップS3 ）、チャネル選択部１５に供給される。

【００４３】チャネル選択部１５は、受信した放送パケットの情報識別子を参照して、各パケットがコンテンツパケット、番組関連情報パケット又は契約関連情報パケットのいずれであるかを判別する（ステップS4 ）。

【００４４】受信パケットがコンテンツパケットである場合には、処理をステップS5 に移行し、現在視聴中のチャネルをチャネルＩ／Ｆ（インタフェース）１６を介して得て（ステップS5 ）、チャネル選択部１５で視聴チャネルのみ限定受信チップ１７のフィルター部１８に送信する。フィルター部１８はコンテンツパケットをデスクランブル部１９に出力する（ステップS6 ）。

【００４５】受信データが番組関連情報パケットである場合には、ステップS7 からステップS8 に処理を移行して、チャネル選択部１５を介して取込まれた番組関連情報パケットは、フィルター部１８によって番組関連情報復号部２６に供給されて、復号が開始される。

【００４６】受信データが契約関連情報パケットである場合には、ステップS9 からステップS10に処理を移行して、チャネル選択部１５からの受信パケットは、フィルター部１８によって契約関連情報認証部２１に供給される。契約関連情報認証譜２１によって、パケット内に含まれる受信装置ＩＤが抽出され、受信装置ＩＤ格納部２２から取り出した受信装置ＩＤと比較することにより、当該契約関連情報パケットが自受信装置向けのものであるか否かを判定する。

【００４７】受信した契約関連情報パケットが自受信装置宛ての契約関連情報である場合には、このパケットは契約情報復号部２４に供給され、そうでなければ処理を終了する。

【００４８】契約関速情報パケットには受信装置個別のマスター鍵によって暗号化されている部分があることから、復号に先だって自受信装置宛てのパケットであるか否かを判定する必要がある。

【００４９】次に、図９のフローチャートを参照して、コンテンツパケットに間する処理について説明する。デスクランブル部１９は、図９のステップS11において、フィルター部１８から供給されたコンテンツパケットのチャネル識別子とチャネルキー識別子とをチャネルキー出力部２８に送信して、チャネルキー出力部２８に対してチャネルキーKchの出力を要請する。

【００５０】チャネルキー出力部２８は契約判定部３０にチャネル識別子を送り、チャネルキーKchの出力の可否を問い合わせる（ステップS12）。契約判定部３０ではこれを受けて、チャネル契約情報格納部２９からチャネル契約関連情報を引き出し（ステップS13）、契約フラグが“１”であれば許可（ステップS16）、“０”であれば不許可の信号（ステップS20）をチャネルキー出力部２８に出力する。

【００５１】チャネルキー出力部２８では送られてきた判定が許可であればチャネルキー格納部２７から当該チャネルのチャネルキー識別子を保持したチャネルキーKchを得てデスクランブル部１９に送信し（ステップS17）、不許可であればコンテンツパケットに関する処理を終了する。

【００５２】なお、ここでコンテンツパケットはパケットの中でも最も多いのでパケット毎に同様の処理を繰り返すと処理に長時間を要する。そこで、同一チャネルの同一チャネルキーKchを用いている限りは、一回チャネルキーKchの出力が許可された場合には、毎回契約判定部３０に問い合わせることなくチャネルキーKchを出力することにより、処理時間を短縮するようになっている。実際には、チャネルキーKchはセキュリティー上の理由で１０秒に１回程度の割合で変更されることから、出力可否の問い合わせを省略しても、限定受信に与える影響は少ない。

【００５３】デスクランブル部１９では チャネルキー

Kchの出力を受けて、コンテンツパケットの暗号化部分を復号し（ステップS18）、コンテンツ出力部２０に出力する（ステップS19）。コンテンツ出力部２０はコンテンツをモニタ等の再生装置に出力して再生させる。

【００５４】受信情報が番組関連情報パケットであった場合には、図８のステップS8 から図１０のステップS21に処理を移行する。番組関連情報復号部２６はフィルター部１８から番組関連情報パケットをが与えられると、チャネル識別子とワーク鍵識別子をキーにして、対応するワーク鍵Kw をワーク鍵格納部２５から取得する。

【００５５】ここで対応するワーク鍵Kw が無い場合には、処理を終了する。ワーク鍵Kwを取得すると、番組関連情報復号部２６は、取得したワーク鍵Kw を用いて番組関連情報を復号する（ステップS22）。復号された番組関連情報の中からチャネルキーKchとそのチャネル識別子を取り出し（ステップS23）、チャネルキー格納部２７へ格納する（ステップS24）。

【００５６】受信情報が契約関連情報であった場合には、図８のステップS10から図１１のステップS31に処理を移行し、契約関連情報認証部２１は、受信装置ＩＤ格納部２２から受信装置ＩＤを抽出する。（ステップS31）。契約関連情報認証部２１は、抽出した受信装置ＩＤと契約関連情報パケットに含まれる受信装置ＩＤとを比較することにより、当該契約関連情報が自受信装置宛てのものであるか否かを判定する（ステップS32）。自受信装置宛てのものでなければ、その時点で処理を終了する。

【００５７】自受信装置宛の契約関連情報を受信した場合には、、契約関連情報認証部２１は、契約関連情報を契約関連情報復号部２４に出力する。契約関連情報復号部２４は、装置個別に設定されているマスター鍵KM をマスター鍵格納部２３から取得し（ステップS33）、契約関連情報パケットの暗号化部分を復号する（ステップS34）。契約関連情報復号部２４は、復号した受信契約関連情報から誤り検出コードを取得し、取得した誤り検出コードを検証することにより当該チャネル契約関連情報が正しいものであるか否かを確認する（ステップS35）。

【００５８】ステップS35の検証処理によって、契約関連情報パケットの中で暗号化されていない受信装置ＩＤを偽造して作成された偽の契約関連情報に基づいて処理が行われることを防止することができる。誤り検出コードは契約関連情報から導出されるものであり、契約関連情報を暗号化したまま改変して偽造しようとしても、復号した際、復号契約関連情報から導出された誤り検出コードと復号によって得られた誤り検出コードとが一致することは極めて稀であり、偽造を確実に防止することができる。なお、仮に誤り検出コードを用いない場合には、暗号化された契約関連情報を適当に改変することにより、復号した結果が元の契約関連情報よりも受信者に有利な条件の契約関連情報に変更可能である可能性が高くなってしまう。

【００５９】誤り検出コードが検証されると、処理をステップS36に移行して、契約関連情報復号部２４は、契約関連情報パケットからワーク鍵Kw とチャネル契約関連情報Cとを取得し（ステップS36，S38）、夫々ワーク鍵格納部２５又は契約情報格納部２９に格納する（ステップS37，S39）。

【００６０】図１において、広域局１は、衛星２を利用して、広域放送を行う。衛星２は広域局１からの放送波を中継して各地域局３，４，…に送信する。各地域局３，４，…は、衛星２からの放送波を受信して、地域内に地域放送を行う。

【００６１】受信端末T1 及び移動受信端末ＭT1 は、図７の受信装置によって構成される。図１の例では、受信端末T1 は固定端末であり、地域局４の加入端末（登録された受信端末）である。また、移動受信端末ＭT1 は、移動端末であり、地域局３，５の加入端末である。図１の移動受信端末ＭT1 ′ は、移動受信端末ＭT1が移動したことを示している。

【００６２】地域局３，４，…は、契約関連情報については、自放送地域内で登録された受信端末宛のみの放送波を受信して中継放送を行うようになっている。

【００６３】即ち、本実施の形態は、衛星放送等の広域放送のみを利用して送信されていた個別受信装置に対する限定情報（契約関連情報）を、受信装置が存在する特定地域のみに向けて放送することにより、限定受信の情報送信量を削減するものである。

【００６４】広域放送局１はコンテンツパケット及び番組関連情報パケットについては、全地域局で中継可能のように、通常の広域放送を行う。一方、契約関連情報パケットについては、各地域局を宛先にして放送を行う。このような契約関連情報の限定受信を可能にするために、広域放送局１は広域局契約管理装置を備えている。

【００６５】図１２は広域放送局１内に設けられた広域局契約管理装置４０の具体的な構成を示すブロック図である。

【００６６】契約内容情報入力部４１は、各契約の内容に応じて、契約ユーザＤＢ（データベース）４２及び地域局ＤＢ４３に情報を入力する。図１３は図１２中の契約ユーザＤＢ４２に蓄積されている情報のフォーマットを示し、図１４は図１２中の地域局ＤＢ４３に蓄積されている情報のフォーマットを示し、図１５は図１２中のワーク鍵ＤＢ４６に蓄積されている情報のフォーマットを示している。

【００６７】契約ユーザＤＢ４２は、図１３に示ように、受信装置ＩＤ、加入している地域局の地域局コードの数ｎとそれに続くｎ個の地域局コード、チャネル契約関連情報を格納している。これらのレコードは当該受信

装置ＩＤを持つ受信装置は地域局コード１～ｎまでの地域局域に存在し、チャネル契約関連情報に示すようなチャネル契約を行なっていることを示している。

【００６８】地域局ＤＢ４３は、図１４に示ように、地域局コード、地域局電話番号、地域局域加入者数ｋ、継続レコード番号からなるレコードを格納している。地域局電話番号は地域局に対して通信を利用する場合に利用する電話番号であり、本実施の形態のように衛星放送によって契約関連情報を送信する場合には、不要である。

【００６９】加入者数ｋは当該地域局コードを含んでいる契約ユーザＤＢ４２内のレコードの数であり、継続レコード番号は当該地域局コードを含む契約ユーザＤＢ４２のレコードのうち直前に送信したレコードの次のレコードが表示される。継続レコード番号は、１日分の送信終了後に更新されるようになっている。

【００７０】送信スケジュール部４４は、地域局ＤＢ４３から各地域局毎に地域局域加入者数ｋを取得する。そして、各地域局に対して、所定の期間、例えば１ヶ月（３０日）で、各地域局の加入者全てに契約関連情報を送信するようにスケジュールを立てる。なお、地域局の加入者数（受信装置数）が少ない場合には、１ヶ月１回よりも頻繁に（例えば１週間に１回）契約関連情報を送信することができる。

【００７１】送信スケジュール部４４は、契約ユーザＤＢ４２から各契約ユーザの情報を読み出して契約関連情報生成部４５に与え、契約関連情報生成部４５は、ワーク鍵ＤＢ４６の内容に従って契約関連情報を作成する。

【００７２】ワーク鍵ＤＢは、図１５に示すように、チャネル識別子、ワーク鍵識別子、ワーク鍵、有効期限の内容を含んでいる。ワーク鍵はワーク鍵識別子を識別子とするチャネル識別子で示されるチャネルのワーク鍵であり、有効期限に示す期間だけ有効であることを示している。

【００７３】契約関連情報生成部４５は、契約ユーザＤＢ４２から抽出したレコードから受信装置ＩＤとチャネル契約関連情報を抽出し、チャネル契約関連情報の中で契約フラグが“１”であるチャネルに対して送信すべきワーク鍵とその識別子及びチャネル識別子をワーク鍵ＤＢ４６から抽出する。ここで送信すべきワーク鍵とは通常現在有効であるワーク鍵と次に有効になるワーク鍵である。

【００７４】契約関連情報生成部４５は、地域局の加入者に送信すべき契約関連情報を地域局送信用契約関連情報生成部４７に出力する。地域局送信用契約関連情報生成部４７は、地域局送信用契約関連情報を作成する。

【００７５】図１６は地域局送信用契約関連情報を示す説明図である。図１６に示すように、地域局送信用契約関連情報は、情報識別子、地域局コード、契約関連情報の数とその数分だけの契約関連情報によって構成されている。ここで、情報識別子は当該パケットが地域局送信用契約関連情報であることを示しており、地域局コードは当該パケットがどの地域局宛てのものであるか否かを表している。更にその地域局域内にある複数の受信端末宛の契約関連情報が配列される。

【００７６】地域局送信用契約関連情報生成部４７によって生成された地域局送信用契約関連情報は、地域局送信用契約関連情報出力部４８に与えられる。地域局送信用契約関連情報出力部４８は、地域局送信用契約関連情報を衛星２を介して送信する。衛星２からの地域局送信用契約管理情報は、地域局３，４，…に設けられた地域局契約管理装置５０によって受信される。

【００７７】図１７は図１中の地域局３，４，…に設けられる地域局契約管理装置５０の具体的な構成を示すブロック図である。

【００７８】地域局契約管理装置５０の受信部５１は、衛星からの放送を受信する。Ａ／Ｄ変換部５２は、受信部５１の受信信号をＡ／Ｄ変換して、誤り検出／訂正部５３に出力する。誤り検出／訂正部５３は、誤り訂正又は検出を行なって、正常なデータのみをフィルター部１８に出力する。フィルター部１８は、当該受信パケットの情報識別子を参照して地域局送信用契約関連情報であるか否かを判定する。

【００７９】フィルター部５４は、地域局コード格納部５５に格納された自局の地域局コードとの比較によって、地域局送信用契約関連情報が自局向けのものであるか否かについても判定する。フィルター部５４は、自局向けの地域局送信用契約関連情報から契約関連情報を抽出して送信ＤＢ５６に出力する。

【００８０】送信ＤＢ５６は、フィルター部５４からの契約関連情報を記憶する。送信ＤＢ５６に登録されているレコードは登録されて１日以上経過すると消去されるようになっており、１日毎に契約管理装置から送信される契約関連情報は全て更新される。

【００８１】送信スケジュール部４４は、送信ＤＢ５６に登録されている契約関連情報を所定のスケジュールに従って送出部５８に出力して、地域放送の限定受信専用チャネル若しくは広域放送の限定受信専用チャネルの合間に暫時繰り返し放送される。

【００８２】次に、このように構成された実施の形態の動作について図１８乃至図２０のフローチャートを参照して説明する。なお、番組関連情報及び放送コンテンツ情報の送信方法は従来と同様であり、説明を省略する。

【００８３】広域局６１内の送信スケジュール部４４は、図１８のステップＳ41において地域局を示すｉを１に初期化した後、地域局ＤＢ４３からｉ番目の地域局レコードを抽出する（ステップＳ42）。次に、送信スケジュール部４４は、抽出した地域局レコードから地域局コードと地域局域加入者数ｋｉを取得する（ステップＳ43）。更にｋｉ／３０とＭとの最大を取ってｍとする（ステップＳ44）。Ｍは１日に最低限送信したい契約関

連情報の数である。即ち、ｋｉ／３０は約１ケ月（３０日）で一回りするための１日分を意味している。

【００８４】従って、このｍを取ることによって、最低限１ヶ月でその地域にある受信装置に送信することを意味している。もちろん当該地域に存在する受信装置が少なければ１ヶ月１回よりも頻繁に（例えば１週間に１回）送信することができる。なお、これらの数値Ｍ，３０は利用形態によって様々に変更されるべきものである。

【００８５】次に、送信スケジュール部４４は、継続レコード番号（図１４）をレコードから抽出し、継続レコード番号に従って、最大m個の地域局コードがついたレコードを契約ユーザＤＢ４２から抽出する（ステップＳ45）。ここで、継続レコードが契約ユーザＤＢ４２の範囲外となった場合には、自動的に契約ユーザＤＢ４２の先頭に戻って抽出を継続する。

【００８６】本実施の形態における継続レコード番号とは、当該地域コードに対応する地域局に対して、当日送信を開始するレコード番号であり、前日に当該地域局に送信したレコードのうち、契約ユーザＤＢ４２上で最後にあたるレコードの次のレコードである。

【００８７】送信スケジュール部４４は、最大m個のレコードを抽出すると、ステップＳ46においてｊ＝１とし、ｊ番目のレコード（登録した受信端末（装置）のレコード）があるか否かを確認する（ステップＳ47）。ｊ番目のレコードが存在する場合には、ステップＳ48において、契約関連情報生成部４５は、ｊ番目のレコードから図１９のアルゴリズムによって契約関連情報を作成する。

【００８８】即ち、契約関連情報生成部４５は、図１９のステップＳ61，Ｓ62において、図１３に示す契約ユーザＤＢ４２から抽出したレコードから受信装置ＩＤとチャネル契約関連情報を抽出し、チャネル契約関連情報の中で契約フラグが“１”であるチャネルに対して送信すべきワーク鍵とその識別子及びチャネル識別子をワーク鍵ＤＢ４６から抽出する（ステップＳ63，Ｓ64）。ここで送信すべきワーク鍵とは通常現在有効であるワーク鍵と次に有効になるワーク鍵である。これらはワーク鍵ＤＢ４６の有効期限情報で知ることができる。

【００８９】例えば、ｉ番目の地域局が図１の地域局５を示すもので、ｊ番目のレコードが受信端末ＭＴ1 を示すものである場合には、この受信端末ＭＴ1 に関する契約関連情報を生成する。

【００９０】次に、ｊをインクリメントして（ステップＳ49）、ステップＳ48，Ｓ48の処理を繰り返す。ステップＳ47おいてｊ番目のレコードが無いことを検出すると、地域局コードを持つ地域局から送信すべき契約関連情報の作成が終了したので、次に地域局に送信するための準備に入る。即ち、ステップＳ50においてｊ＝０でないことを確認した後、ステップＳ51において地域局送信用契約関連情報を作成する。

【００９１】地域局送信用契約関連情報生成部４７は、図１６に示す地域局送信用契約関連情報を作成する。地域局送信用契約関連情報は、図１６に示すように、情報識別子、地域局コード、契約関連情報の数とその数分だけの契約関連情報によって構成されている。ここで、情報識別子は当該パケットが地域局送信用契約関連情報であることを示しており、地域局コードは当該パケットがどの地域局宛てのものであるか否かを表している。更にその地域局域内にある受信装置の契約関連情報がその総数の後に続く。

【００９２】地域局送信用契約関連情報生成部４７によって生成された地域局送信用契約関連情報は、次のステップＳ52において、地域局送信用契約関連情報出力部４８から送信される。なお、ステップＳ50の判断時にｊ＝０である場合には、ｉ番目の地域局域内には受信装置が存在しないことを意味するので送信のための処理を行なわず、ｉ＝ｉ＋１として次の地域局の処理に移る（ステップＳ53）。

【００９３】こうして、図１の各地域局３，４，…の受信端末Ｔ1 ，ＭＴ1 （ＭＴ1 ′）についての契約関連情報も、これらの端末を加入者とする地域局宛に図１６の地域局送信用契約関連情報の放送が行われる。

【００９４】ｉ番目の地域局送信用契約関連情報の送信が終了したら、Ｎを地域局の総数としてｉ＝ｉ＋１としてｉ＜Ｎであるか否かを判断する（ステップＳ54）。ｉ＜Ｎであれば次の地域局域内の受信装置に関して同様の操作を繰り返す。ｉ＞＝Ｎの場合には、地域局ＤＢ４３に登録されている地域局に関して、１日分の送信操作が終了したことになるので、図１８のフローを終了し、翌日また起動する。

【００９５】一方、地域局３，４，…においては、地域局契約管理装置５０の受信部５１において、衛星からの放送を受信する（図２０のステップＳ71）。Ａ／Ｄ変換部５２は、受信部５１の受信信号をＡ／Ｄ変換して（ステップＳ72）誤り検出／訂正部５３に出力する。誤り検出／訂正部５３は、誤り訂正又は検出を行なって（ステップＳ73）、正常なデータのみをフィルター部１８に出力する。フィルター部１８は、当該受信パケットの情報識別子を参照して地域局送信用契約関連情報であるか否かを判定する（ステップＳ74）。

【００９６】地域局送信用契約関連情報でなかった時は、そのパケットの処理を終了する。地域局送信用契約関連情報であった場合には、ステップＳ75において、自局向けのものであるか否かを判定する。自局向けでなければ処理を終了する。自局向けであれば、当該パケットに含まれている契約関連情報を抽出して、送信ＤＢ５６に登録する（ステップＳ76）。

【００９７】ここで送信ＤＢ５６に登録されているレコードは登録されて１日以上経過すると消去されるように

構成されている。このため、１日毎に契約管理装置から送信される契約関連情報が全て更新される。

【００９８】送信ＤＢ５６に登録されている契約関連情報は、送信スケジュール部５７によって指示されたスケジュールに従って地域放送の限定受信専用チャネル若しくは広域放送の限定受信専用チャネルの合間に暫時繰り返し放送される。（ステップS77）。

【００９９】こうして、受信端末T1 は地域局４から放送された契約関連情報を受信し、移動受信端末ＭＴ１，（ＭＴ１′）は地域局５，３から契約関連情報を受信する。１受信端末であっても複数の地域局に登録することによって、登録した複数の地域局から契約関連情報を取得することができ、移動端末であっても、登録した地域局の放送範囲内であれば、限定受信が可能である。

【０１００】このように、本実施の形態においては、各受信機が受信すべき番組関連情報、放送コンテンツ情報及び契約関連情報のうち、限定受信の対象となる契約関連情報については、対応する地域局のみから送信するようになっている。これにより、契約関連情報の送信量を削減することができる。

【０１０１】契約関連情報の送信量の削減により、同じ帯域幅であれば各契約者に対する契約関連情報の送信頻度を上げることができる。このことは例えば前述したモバイル放送の場合特に有効である。何故ならモバイル放送における受信装置は（車庫に入ったり等して）常に受信状態にあるとは言えない。このため受信情報になった再、タイムリーに契約関連情報を受信することができる本発明は有用である。

【０１０２】図１の実施の形態においては、広域局が衛星を利用して契約関連情報を地域局に送信する例について説明した。広域局から地域局への契約関連情報の送信に、通信を利用することも考えられる。

【０１０３】図２１はこの場合の実施の形態を示す説明図であり、契約関連情報を広域局から地域局に通信を利用して送信する例を示している。図２１において、広域局６１は、図示しない衛星等を利用して広域放送を行うと共に、限定受信情報については、地域局６２，６３，…に対して所定の通信路を介した通信が可能である。各地域局６２，６３，…は、衛星等から広域放送の放送波を受信して地域内に地域放送を行うと共に、通信路を介して通信によって限定受信情報を受信して、地域内に地域放送を行うことができるようになっている。

【０１０４】ところで、地域局６２，６３，…へのデータの送信は、地域局の電話番号とプロトコルさえ知っていればだれでも可能である。従って、善意悪意に拘わらず誤ったデータが地域局６２，６３，…に送信されて、そのまま放送されてしまう危険がある。

【０１０５】このため、地域局６２，６３，…は、公衆通信網を利用した契約関連情報の送受信において、受信したデータが確かに広域局から送られてきたものか否かを確認する必要がある。そこで、本実施の形態では、広域局６１から地域局６２，６３，…に送信データを送る際に、データにデジタル署名を付加し、地域局６２，６３，…が広域局６１から該送信データを受信する際に付随しているデジタル署名を検証することによって、広域局６１からのデータであることを確認するようになっている。

【０１０６】図２２は図２１中の広域局６１に設けられる広域局契約管理装置７１の具体的な構成を示すブロック図である。図２２において図１２と同一の構成要素には同一符号を付して説明を省略する。

【０１０７】図２２の広域局契約管理装置７１は、地域局送信用契約関連情報生成部４７に署名生成鍵格納部７２が付随する点が図１２の広域局契約管理装置４０と異なる。署名生成鍵格納部７２は、署名生成鍵を格納しており、地域局送信用契約関連情報生成部４７は、地域局送信用契約関連情報を生成する際に図１６に示す地域局送信用契約関連情報の契約関連情報の数から契約関連情報までの部分について、署名生成鍵格納部７２に格納されている署名生成鍵によってデジタル署名を作成するようになっている。地域局送信用契約関連情報生成部４７は、図２３に示すように、地域局送信用契約関連情報の最後に、作成したデジタル署名を付加して地域局送信用契約関連情報出力部４８に出力する。

【０１０８】図２４は図２１中の地域局６２，６３，…に設けられる地域局契約管理装置８１の具体的な構成を示すブロック図である。図２４において図１７と同一の構成要素には同一符号を付して説明を省略する。

【０１０９】モデム部８２は、通信路を介して伝送された情報を受信して、地域局コード検証部８３に出力する。地域局コード格納部５５には自地域局のコードが格納されている。地域局コード検証部８３は、受信した情報中の地域局コードと地域局コード格納部５５に格納されている地域局コードとが一致することによって自局宛の情報であるものと判断する。

【０１１０】地域局コード検証部８３は、受信情報を署名検証部８５に出力する。署名検証鍵格納部８６は、署名検証鍵を格納しており、署名検証部８５は、受信情報に含まれるデジタル署名を署名検証鍵で検証することによって署名検証を行う。正しく署名検証された場合にのみ、署名検証部８５は受信データの契約関連情報を送信ＤＢ５６に出力するようになっている。

【０１１１】次に、このように構成された実施の形態の動作について図２５のフローチャートを参照して説明する。図２５において図２０と同一の手順には同一符号を付して説明を省略する。

【０１１２】広域局６１の広域局契約管理装置７１は、地域局送信用契約関連情報を生成する場合には、地域局送信用契約関連情報の契約関連情報の数から契約関連情報までの部分について署名生成鍵格納部７２に格納され

ている署名生成鍵によってデジタル署名を作成し、地域局送信用契約関連情報の最後に付加して出力する。他の作用は図１２の広域局契約管理装置４０と同様である。

【０１１３】一方、地域局契約管理装置８１においては、モデム部８２において公衆回線からの情報を受信する（ステップS71）。受信された情報は地域局送信用契約関連情報であることが確認された後（ステップS74）、地域局コード検証部８３に供給される。受信された情報が地域局送信用契約関連情報ではなかった場合には当該情報に関する処理を終了する。

【０１１４】地域局コード検証部８３は地域局送信用契約関連情報パケットに含まれる地域局コードが自局のものか否かをチェックする（ステップS75）。地域局コードが自局のものでなければ処理を終了し、自局のものであれば、当該パケットを署名検証部８５に出力する。署名検証部８５では、デジタル署名の検証が行なわれる（ステップS81）。署名検証に失敗した場合には処理を終了する。デジタル署名が検証された場合には、パケットの中から契約関連情報の数だけ契約関連情報を抽出し、送信ＤＢ５６に登録する（ステップS76）。送信ＤＢ５６に登録されている契約関連情報は放送スケジュール部５７からのスケジュールに従って地域放送の限定受信専用チャネル若しくは広域放送の限定受信専用チャネルの合間に暫時繰り返し放送される。（ステップS77）。

【０１１５】このように、本実施の形態においても図１の実施の形態と同様の効果を得ることができる。

【０１１６】なお、上記図１の実施の形態においては、広域局から地域局に衛星放送によって地域局送信用契約関連情報を送信する場合にはデジタル署名の生成及び検証を行なっていないが、図２１の実施の形態と同様の構成によって、デジタル署名を導入することができることは明らかである。この場合には、衛星放送による地域局送信用契約関連情報の送信をより確実なものにすることができる。

【０１１７】また、逆に、広域局と地域局の間に専用線が設けられていること等によって他から通信される恐れがない場合には、通信による送信であってもデジタル署名の必要はない。このように上記各実施の形態は利用形態によって様々変更可能である。

【０１１８】また、広域局から地域局への送信をより確実にするためには、衛星放送による送信と通信による送信とを併用するシステムが望ましい。このような構成は、図１及び図２１において、広域局にあっては送信部を、地域局にあっては受信部を２つ備えることによって可能であり、処理の流れも２つの場合に分けてそれぞれ上述した処理を行なうことによって容易に構成することができる。

【０１１９】また、上記各実施の形態における地域局としては人的介入が全くなく全て自動的に行なうよう構成することができることから、地域向けの番組を放送する局ばかりでなく、単に電波増幅のための中継局であってもよい。即ち、中継局としてはモバイル放送等で利用されるギャップフィラーでも構わないし、地域局として移動局を採用することも可能である。このように本実施の形態では地域局として（無人有人の別なく）地域放送システムを利用することが可能である。

【０１２０】また、上記各実施の形態では、各受信装置に対して契約関連情報を送信する地域局に関しては特に限定していなかったが、据え置き型の受信装置の場合は設置場所が局域に入るような地域局１局から送信すればよいが、車載受信装置のようなモバイル環境下にある受信装置に対しては複数の地域局から契約関連情報を送信する必要がある。このため、モバイル受信装置での受信を前提とした放送システムにおいては広域局側の契約管理装置の契約ユーザＤＢの地域局コードには複数の地域局コードが登録できるように構成するのが望ましい。更に、モバイル放送においては例えば高速道路を日夜走るトラックのように移動経路がはっきりしている受信装置向けに高速道路上にある地域局を全て束にして扱うように地域局コードを構成したり、地域局コードは別々でも処理の中で一括して送信するような工夫が望まれる。

【０１２１】また、地域局としてギャップフィラー等狭い範囲に対してのみ有効な中継局を利用すると地域の限定が強くなり、受信装置に対する契約関連情報の送信効率が上がる反面で、広域局から地域局送信用契約関連情報を送信する中継局の数が多くなり、広域局からの送信に長時間を要する等の不都合が生ずる。

【０１２２】そこで、図２６に示す階層構造を利用する方法が考えられる。図２６に示すように、地域局の中に親局９２，９３，…と子局A1 ～An ，B1 ～Bm ，C1 ～Cu を設け、広域局９１からは親局９２，９３，…に対して、親局９２，９３，…の支配下にある子局A1 ～An ，B1 ～Bm ，C1 ～Cu に送信する契約関連情報を送信し、各親局９２，９３，…が支配下の子局A1 ～An ，B1 ～Bm ，C1 ～Cu に対して、それぞれのデータを送信するような構成をとることが望ましい。同様に子局A1 ～An ，B1 ～Bm ，C1 ～Cu が更に孫局に送信する場合も考えられ、この場合には一層効率を向上させることができる。このような構成における認証は、子局が広域局の認証を行なうような構成にしてもよく、また、直接親局を認証するように構成してもよい。特に、広域局と親局の間が専用線で接続され、認証の必要がない場合等には後者が有効となる。

【０１２３】また、図２１の実施の形態では、通信で地域局送信用契約関連情報を送信する際、広域局から地域局に向けて通信しているが、この逆でも構わない。但し、この場合には、広域局はどこから電話が掛かってきたか分からないことがあるので、広域局が地域局を認証する必要がある。この場合の認証は、チャレンジ・レス

ポンス型の認証を用いればよい。更に、図２１の実施の形態における地域局が広域局を認証する認証方式にもチャレンジ・レスポンス型の認証を行なうこともできる。

【０１２４】更に本実施の形態では、本発明の構成を明らかにするため契約関連情報を地域局から送信する場合のみを述べてきたが、これを現行の広域局からの送信と併用しても構成上矛盾は生じない。この場合２つの方式が考えられる。１つは広域局からの限定受信情報送信の合間に地域局からの契約関連情報の送信を挟む方式。もう１つは（広域局からの送信を前提とする）従来の限定受信チャネルの他に地域放送から契約関連情報を送信するため限定受信チャネルを創設し、後者のチャネルで前記実施の形態で述べた方式で契約関連情報を送信する方式である。

【０１２５】また、このように広域放送による契約関連情報の送信と、地域放送による契約関連情報の送信を併用すると、引越しその他の理由により、受信装置の受信エリアが変更された場合でも、十分対応できるという利点がある。

【０１２６】図２７乃至図３３は本発明の他の実施の形態に係り、図２７は鍵構成を示す説明図、図２８は契約関連情報パケットを示す説明図、図２９は契約関連情報を示す説明図、図３０は受信装置の構成を示すブロック図、図３１乃至図３３は受信装置の動作を説明するためのフローチャートである。

【０１２７】図１及び図２１の実施の形態においては、受信装置に固有のマスター鍵を用いる限定受信システムに適用した例であったが、本実施の形態は全ての受信装置が共通のマスター鍵を有する限定受信システムに適用した例である。本実施の形態のハード構成は、図１又は図２１の実施の形態と同様であり、図示を省略する。

【０１２８】このような限定受信システムにおいては各受信装置に対して、個別に契約関連情報を暗号化して送信する必要がないので限定受信情報の送信量が少なくてすむという利点がある。しかし、マスター鍵が不正に取得された場合には被害範囲が大きいという安全性の問題を有する。そこで、デジタル署名等の偽造防止技術を用いて対策する必要がある。なお、以下に述べる方式は、電気通信技術審議会資料「２．６ＧＨｚ帯の電波を利用する衛星デジタル音声放送システムの技術的条件」に基づく方式を簡明に説明したものである。

【０１２９】本実施の形態においては、図２７に示すように、２段の鍵構成を採用する。即ち、放送コンテンツをチャネルキーＫchでスクランブルを施すと共に、チャネルキーＫchとチャネル契約関連情報とを全ての受信装置に共通のマスター鍵ＫＭ で暗号化して送信する。送信されたチャネルキーＫchを用いて放送コンテンツを復号する。

【０１３０】本実施の形態の限定受信システムにおいて放送受信装置が受信するデータは、コンテンツパケット及び契約関連情報パケットの２種類である。コンテンツパケットは、図３と同一の形式を有する。一方、契約関連情報パケットは図２８に示す形式を有する。

【０１３１】即ち、コンテンツパケットは、図３に示すように、情報識別子、チャネル識別子、チャネルキー識別子、放送コンテンツによって構成されており、放送コンテンツはチャネルキーＫchによって暗号化されている。各情報の意味と役割は図１の実施の形態と同一である。

【０１３２】契約関連情報パケットは、図２８に示すように、情報識別子、マスター鍵識別子、チャネル識別子、チャネルキー識別子、チャネルキー、契約関連情報の数ｎ、ｎ個の契約関連情報及びデジタル署名によって構成されている。チャネル識別子からデジタル署名までの部分はマスター鍵で暗号化される。デジタル署名は、契約関連情報数ｎから契約関連情報ｎまでの部分に関してのデジタル署名である。デジタル署名は契約関連情報の偽造を防ぐためのものであり、契約関連情報を１ビットでも変更するとデジタル署名が検証できなくなるという性質を有する。また、デジタル署名を作成するには放送局側にしか存在しない秘密鍵を知る必要があり、デジタル署名を付加することによって契約関連情報の偽造を防止することができる。

【０１３３】契約関連情報は、図２９に示すように、受信装置ＩＤとチャネル契約関連情報とから構成されており、受信装置ＩＤに対応するチャネル契約関連情報を表している。契約関連情報に含まれるその他の情報は、図１の実施の形態に示されている対応する情報と同一の意味と役割を有する。

【０１３４】このように構成された実施の形態においては、コンテンツパケットは各地域局において同一内容が広域に放送される。一方、契約関連情報パケットについては、各地域局の加入者宛に地域放送される。

【０１３５】図３０は本実施の形態において採用される受信機の構成を示している。図３０において図７と同一の構成要素には同一符号を付して説明を省略する。また、図３１乃至図３３において図８、図９及び図１１と同一の手順には同一符号を付して説明を省略する。

【０１３６】図３０の放送受信装置は、受信部１２において放送波を受信後（図３１のステップＳ1 ）、Ａ／Ｄ変換部１３にてＡ／Ｄ変換を行なって（ステップＳ2 ）デジタルデータに変換する。次に、ステップＳ3 において、誤り検出／訂正部１４は、誤り検出及び誤り訂正を行なう。フィルター部１８は、パケット内の情報識別子によってコンテンツパケットであるか否かを判断し（ステップＳ4 ）、そうであればチャネル識別子を参照して、視聴チャネルのコンテンツか否かを判定する（ステップＳ5 ）。視聴チャネルであった場合には、ステップＳ6 でコンテンツパケットはデスクランブル部１９に供給される。そうでない場合には、当該パケットに関する

処理を終了する。契約関連情報パケットであった場合には、フィルター部１８はステップS9 からステップS10に処理を移行して、契約関連情報パケットを契約関連情報復号部２４に供給する。

【０１３７】視聴チャネルのコンテンツパケットの処理は、図１の実施の形態と同様である。契約関連情報パケットの処理は、図３３のフローチャートに従って行われる。即ち、契約関連情報が契約関連情報復号部２４に入力されると、契約関連情報復号部２４はマスター鍵識別子をキーにして、マスター鍵格納部２３からマスター鍵KM を取得して（ステップS33）、暗号化部分を復号する（ステップS34）。契約関連情報復号部２４は、復号された契約関連情報からチャネルキー、チャネル識別子、チャネルキー識別子を抽出し（ステップS90）、チャネルキー格納部２７に格納する（ステップS91）。

【０１３８】次に、契約関連情報復号部２４は、契約関連情報数ｎからデジタル署名までの部分を契約情報認証部２１に出力する。契約情報認証部２１は契約関連情報数ｎを抽出し、それを変数ＭＡＸに代入する（ステップS92）。契約情報認証部２１は、最後の契約関連情報の認証が終わるまで引続き契約関連情報を次々参照する（ステップS94）。

【０１３９】契約情報認証部２１は、ステップS95において契約関連情報が自装置宛のものであるか否かを判定し、自装置宛のものである場合には、デジタル署名を検出する（ステップS97）。契約関連情報復号部２４は、デジタル署名を検証後に、対応するチャネル契約関連情報Ｃを契約情報格納部２９へ格納する（ステップS99）。自受信装置の受信装置ＩＤと一致する契約関連情報がない場合やデジタル署名が検証できなかった場合には、当該パケットに関する処理を終了する。

【０１４０】このように、本実施の形態においても、図１及び図２１の実施の形態と同様の効果を得ることができる。

【０１４１】本実施の形態の限定受信方式ではワーク鍵を用いておらずマスター鍵が共通であることから、解約等視聴しなくなるチャネルが生じた場合には受信装置に格納されているチャネル契約関連情報を更新する必要がある。このため、当該受信装置に確実に契約関連情報を受信させる仕組みが必要であり、送信される地域を限定することにより頻繁に契約関連情報を送信可能とした本実施の形態は極めて有用である。

【０１４２】なお、本実施の形態においても、図１及び図２１の実施の形態で述べた種々の変形を同様に構成可能である。

【０１４３】

【発明の効果】以上説明したように本発明によれば、限定受信に必要な情報の放送を効率化することにより、送信量の増大を抑制することができるという効果を有する。

【図面の簡単な説明】

【図１】本発明に係る限定受信システムの一実施の形態を示す説明図。

【図２】コンテンツパケットのパケット形式を示す説明図。

【図３】番組関連情報パケットのパケット形式を示す説明図。

【図４】契約関連情報パケットのパケット形式を示す説明図。

【図５】ワーク鍵情報の形式を示す説明図。

【図６】チャネル契約関連情報を示す説明図。

【図７】受信装置の全体構成を示すブロック図。

【図８】受信装置の作用を説明するためのフローチャート。

【図９】受信装置の作用を説明するためのフローチャート。

【図１０】受信装置の作用を説明するためのフローチャート。

【図１１】受信装置の作用を説明するためのフローチャート。

【図１２】広域放送局１内に設けられた広域局契約管理装置４０の具体的な構成を示すブロック図。

【図１３】図１２中の契約ユーザＤＢ４２に蓄積されている情報のフォーマットを示す説明図。

【図１４】図１２中の地域局ＤＢ４３に蓄積されている情報のフォーマットを示す説明図。

【図１５】図１２中のワーク鍵ＤＢ４６に蓄積されている情報のフォーマットを示す説明図。

【図１６】地域局送信用契約関連情報を示す説明図。

【図１７】図１中の地域局３，４，…に設けられる地域局契約管理装置５０の具体的な構成を示すブロック図。

【図１８】実施の形態の動作を説明するためのフローチャート。

【図１９】実施の形態の動作を説明するためのフローチャート。

【図２０】実施の形態の動作を説明するためのフローチャート。

【図２１】本発明の他の実施の形態を示す説明図。

【図２２】図２１中の広域局６１に設けられる広域局契約管理装置７１の具体的な構成を示すブロック図。

【図２３】地域局送信用契約関連情報を示す説明図。

【図２４】図２１中の地域局６２，６３，…に設けられる地域局契約管理装置８１の具体的な構成を示すブロック図。

【図２５】実施の形態の動作を説明するためのフローチャート。

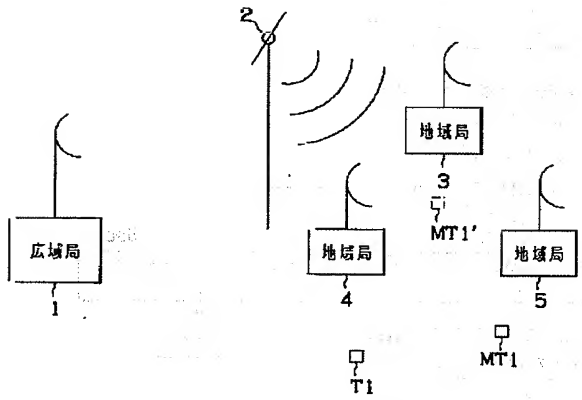
【図２６】階層構造を利用した実施の形態を示す説明図。

【図２７】図２７は鍵構成を示す説明図。

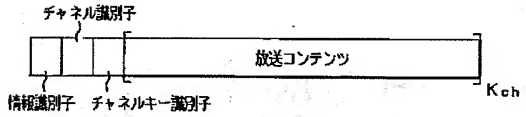
【図２８】図２８は契約関連情報パケットを示す説明

図。
【図２９】図２９は契約関連情報を示す説明図。
【図３０】図３０は受信装置の構成を示すブロック図。
【図３１】受信装置の動作を説明するためのフローチャート。
【図３２】受信装置の動作を説明するためのフローチャート。
【図３３】受信装置の動作を説明するためのフローチャート。
【図３４】デジタル放送において採用される限定受信を可能にする鍵構成の一例を示す説明図。
1…広域局、2…衛星、3〜5…地域局。

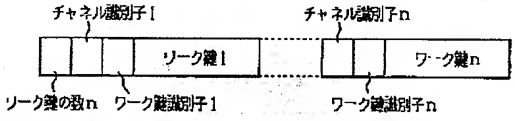
【図１】



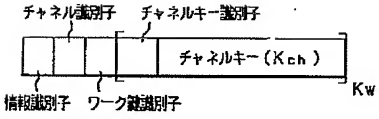
【図２】



【図５】

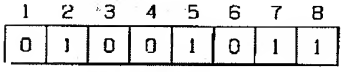


【図３】

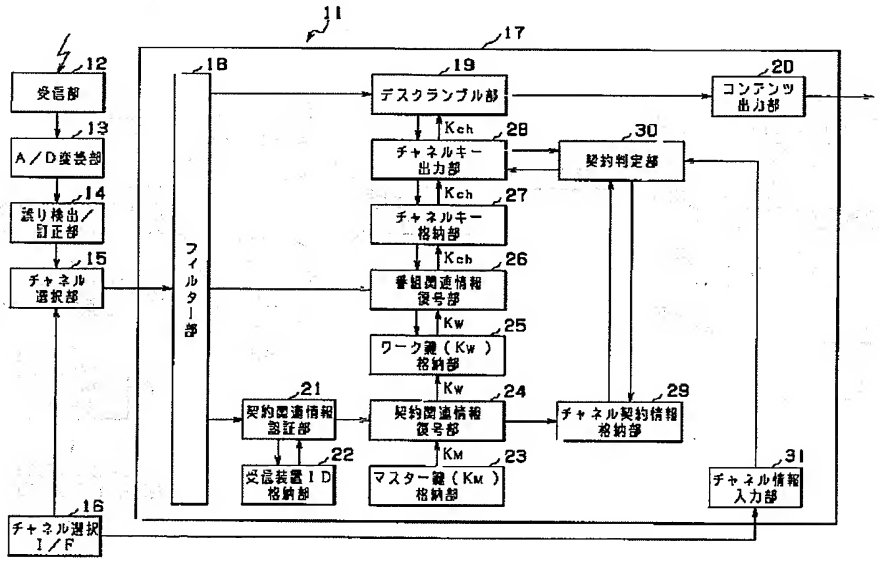


【図４】

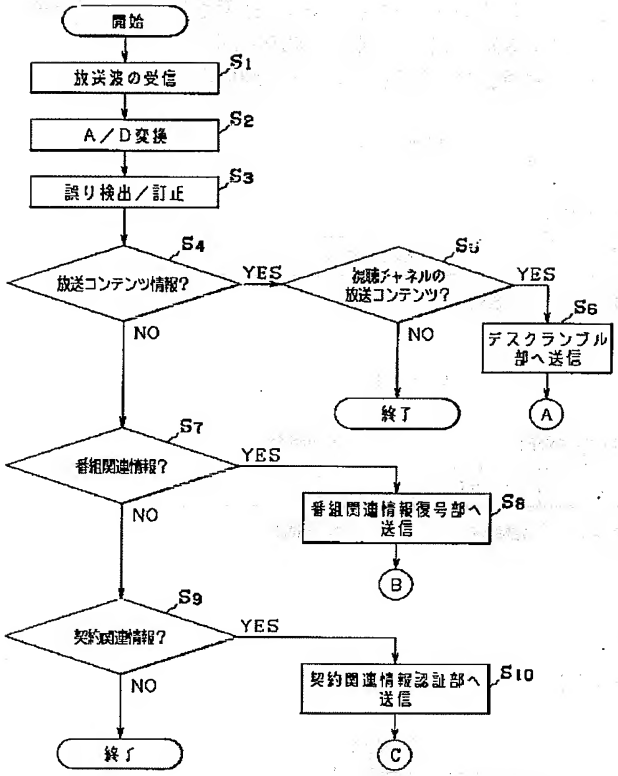
【図６】



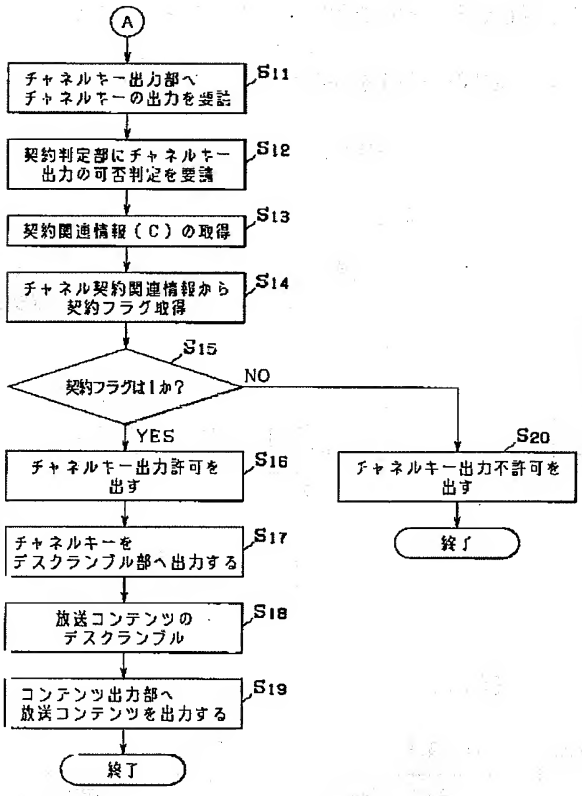
【図７】



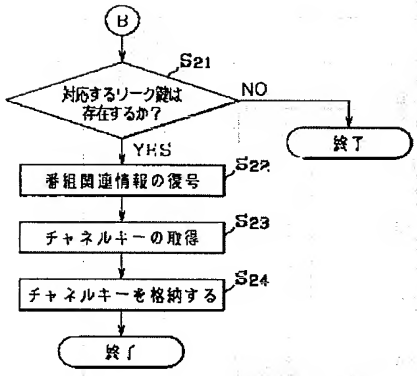
【図８】



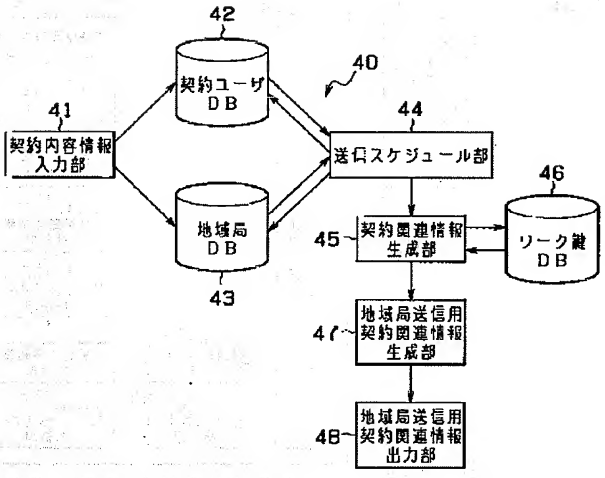
【図９】



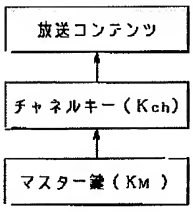
【図１０】



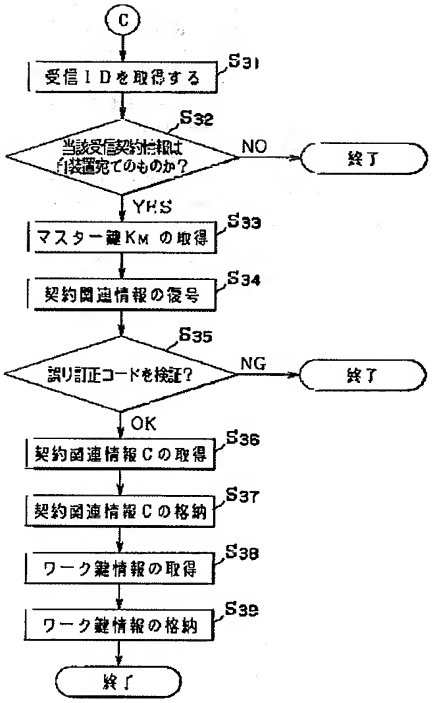
【図１２】



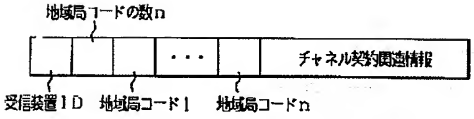
【図２７】



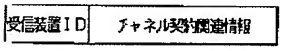
【図11】



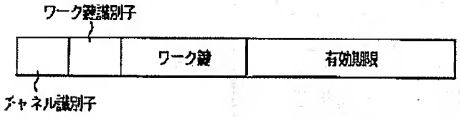
【図13】



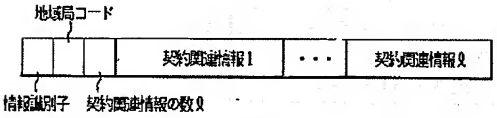
【図29】



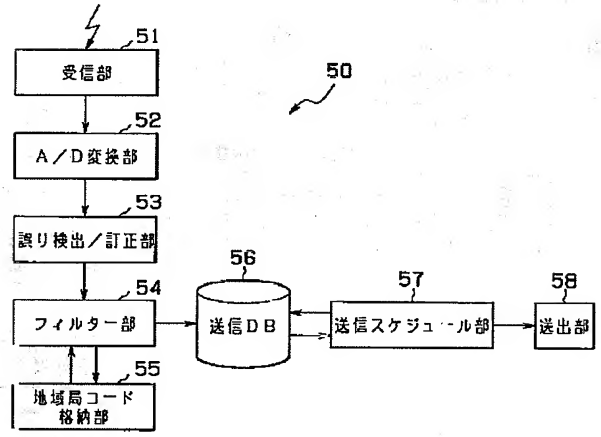
【図15】



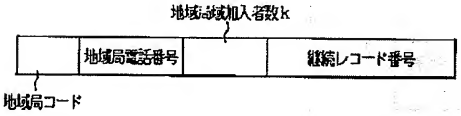
【図16】



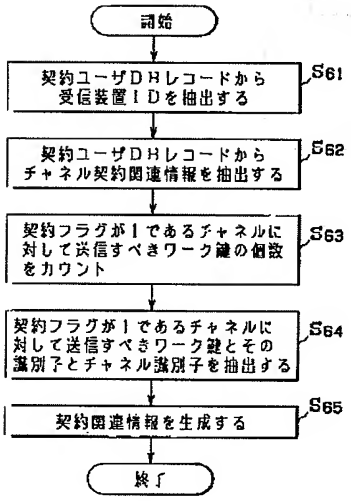
【図17】



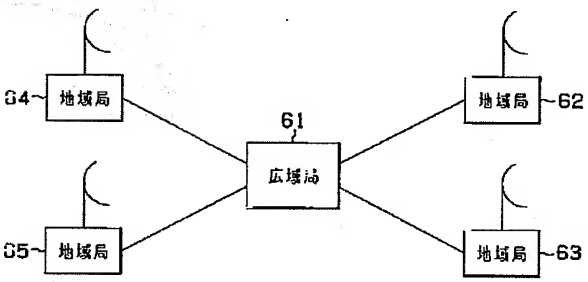
【図14】



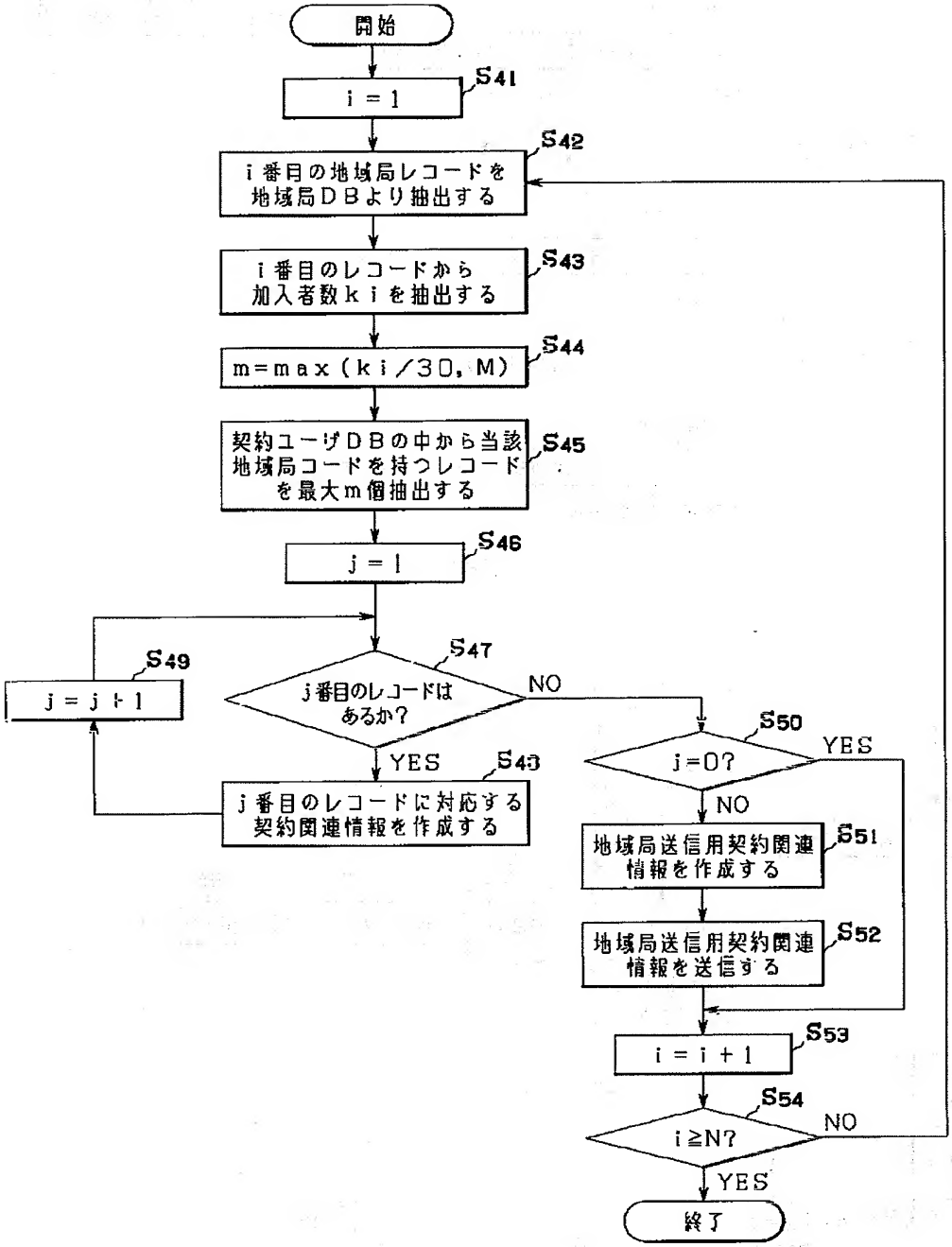
【図19】



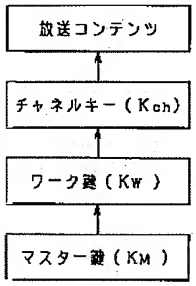
【図21】



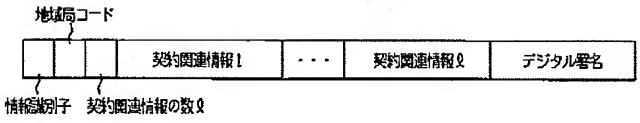
【図１８】


開始
i = 1
S41
i番目の地域局レコードを地域局ＤＢより抽出する
S42
i番目のレコードから加入者数ｋｉを抽出する
S43
m=max(ki/30, M)
S44
契約ユーザＤＢの中から当該地域局コードを持つレコードを最大m個抽出する
S45
j = 1
S46
j番目のレコードはあるか?
S47
NO
YES
j番目のレコードに対応する契約関連情報を作成する
S48
j = j + 1
S49
j=0?
S50
YES
NO
地域局送信用契約関連情報を作成する
S51
地域局送信用契約関連情報を送信する
S52
i = i + 1
S53
i≧N?
S54
NO
YES
終了

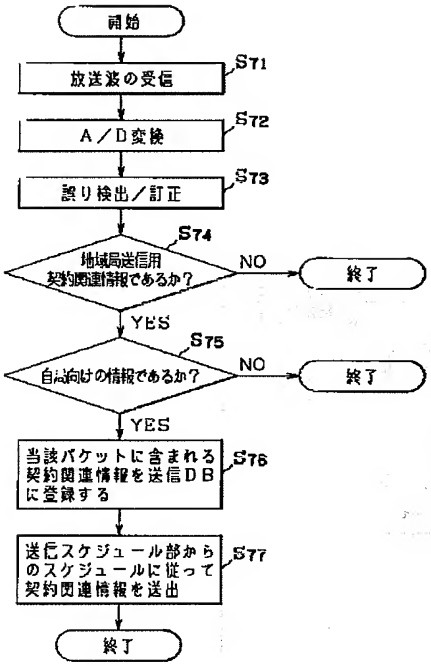
【図３４】


放送コンテンツ
チャネルキー(Kch)
ワーク鍵(Kw)
マスター鍵(KM)

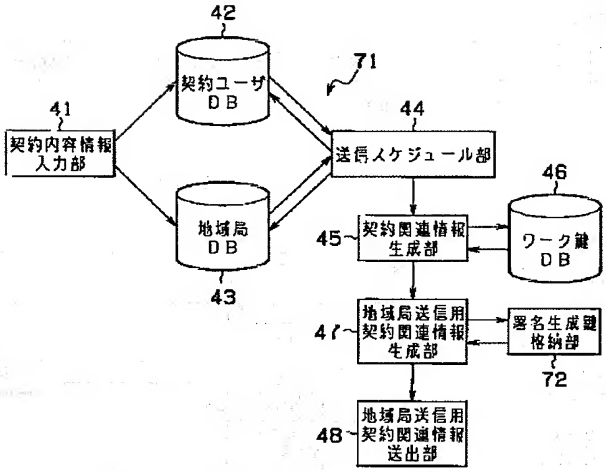
【図２３】


地域局コード
契約関連情報1
・・・
契約関連情報k
デジタル署名
情報識別子
契約関連情報の数k

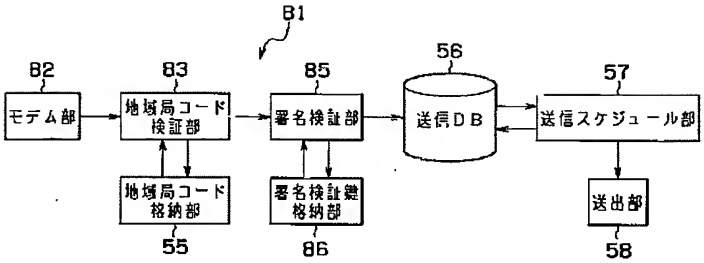
【図20】



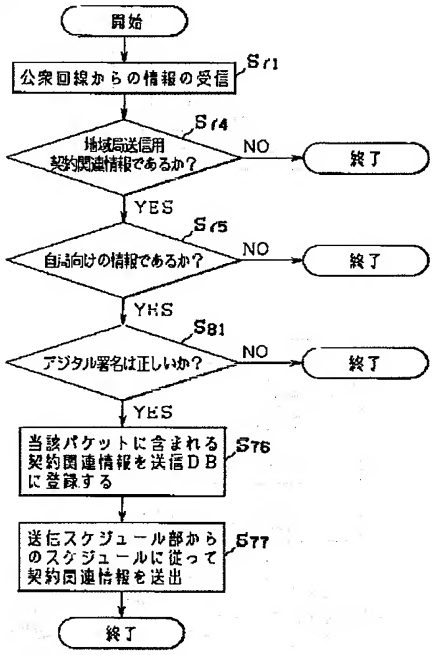
【図22】



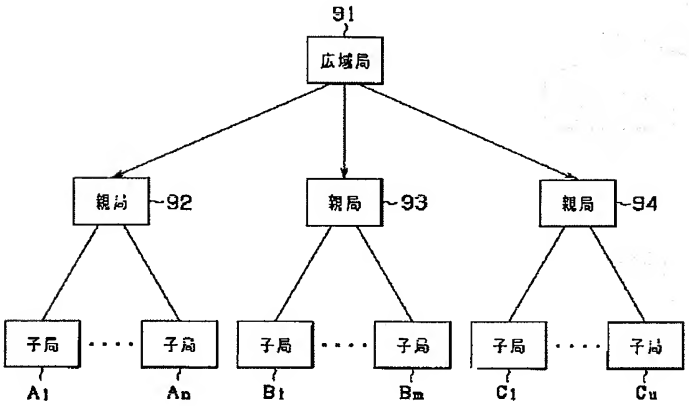
【図24】



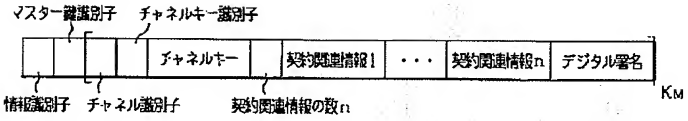
【図25】



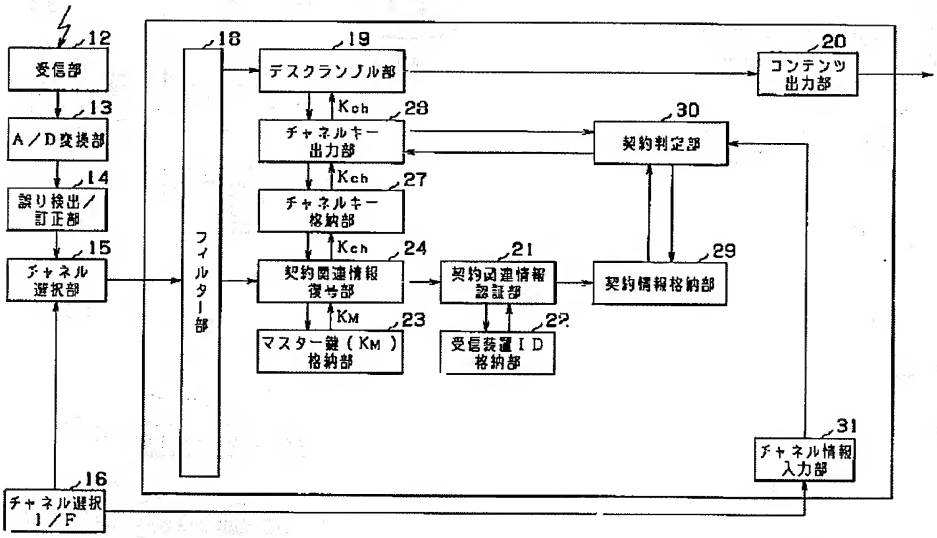
【図26】



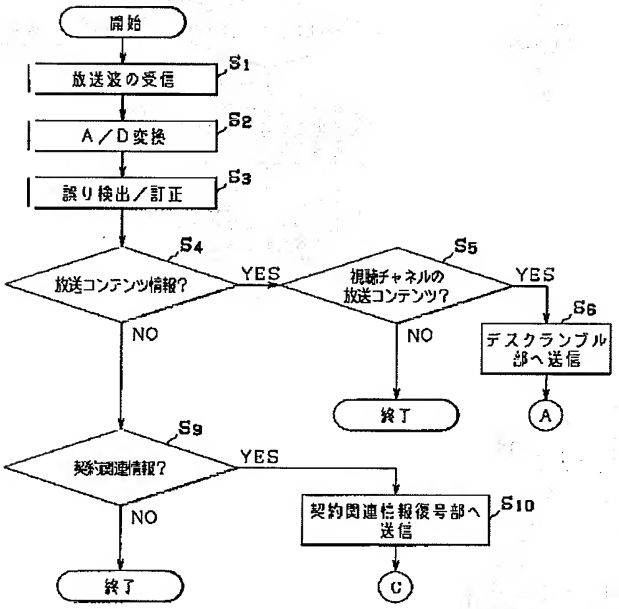
【図２８】


マスター鍵識別子
チャネルキー識別子
チャネルキー
契約関連情報1
・・・
契約関連情報n
デジタル署名
KM
情報識別子
チャネル識別子
契約関連情報の数n

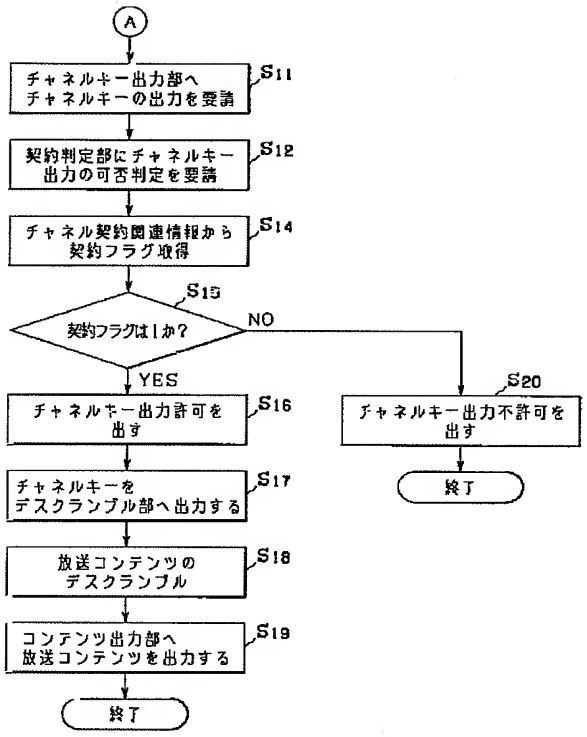
【図３０】


12
受信部
13
A／D変換部
14
誤り検出／訂正部
15
チャネル選択部
16
チャネル選択I／F
18
フィルター部
19
デスクランブル部
20
コンテンツ出力部
Kch
28
チャネルキー出力部
30
契約判定部
Kch
27
チャネルキー格納部
Kch
24
契約関連情報復号部
21
契約関連情報認証部
29
契約情報格納部
KM
23
マスター鍵（KM）格納部
22
受信装置ID格納部
31
チャネル情報入力部

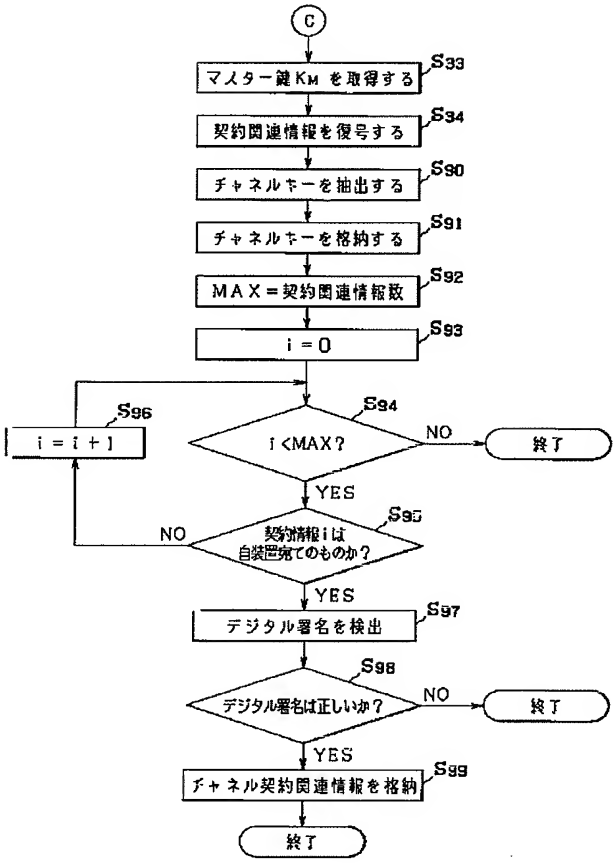
【図３１】


開始
放送波の受信
S1
A／D変換
S2
誤り検出／訂正
S3
放送コンテンツ情報?
S4
YES
視聴チャネルの放送コンテンツ?
S5
YES
S6
デスクランブル部へ送信
NO
NO
終了
A
契約関連情報?
S9
YES
契約関連情報復号部へ送信
S10
NO
終了
C

【図32】



【図33】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
		H04L 9/00	601E	

Fターム(参考) 5C064 BA01 BB02 BB07 BC07 BC17
BC22 BD07 BD08
5J104 AA04 AA07 AA09 AA16 BA03
EA06 EA18 EA26 KA02 NA02
NA03 NA42 PA05